(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/039100 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/JP2004/015752

(22) International Filing Date: 18 October 2004 (18.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003-356073 16 October 2003 (16.10.2003) JP

(71) Applicant *(for all designated States except US)*: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501 (JP).

(71) Applicant *(for US only)*: YAMAMICHI, Masami (heir of the deceased inventor).

(72) Inventor: YAMAMICHI, Masato (deceased).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FUTA, Yuichi. OHMORI, Motoji. TATEBAYASHI, Makoto.

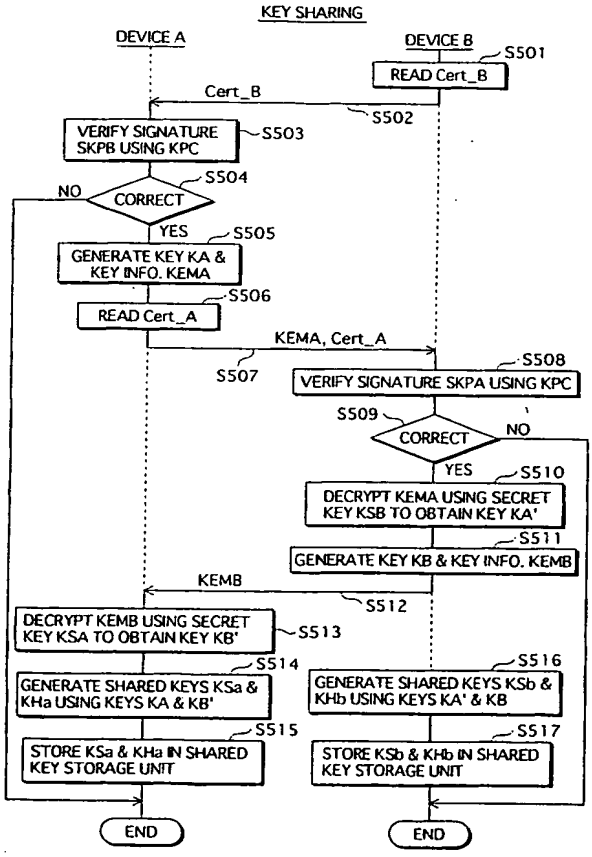
(74) Agent: NAKAJIMA, Shiro; 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072 (JP).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: ENCRYPTED COMMUNICATION SYSTEM AND COMMUNICATION DEVICE



(57) Abstract: In an encrypted communication system that includes a first and a second device, the first device encrypts a 1st key using a public key of the second device to generate 1st encrypted data, which is then transmitted to the second device, receives 2nd encrypted data from the second device, which is then decrypted using a secret key of the first device to obtain a 2nd key, and generates, based on the 1st and 2nd keys, a 1st encryption key for use in communication with the second device. The second device encrypts a 3rd key using a public key of the first device to generate the 2nd encrypted data, which is then transmitted to the first device, receives the 1st encrypted data, which is then decrypted using a secret key of the second device to obtain a 4th key, and generates, based on the 3rd and 4th keys, a 2nd encryption key for use in communication with the first device. The first and second devices perform encrypted communication using the 1st and 2nd encryption keys.

WO 2005/039100 A1

ATTACHMENT A

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.